The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

9/9/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR Could Allow Remote Code Execution (APSB14-21)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Adobe AIR is a cross platform runtime used for developing Internet applications that run outside of a browser.

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

Adobe Flash Player 14.0.0.179 and earlier versions
Adobe Flash Player 13.0.0.241 and earlier 13.x versions
Adobe Flash Player 11.2.202.400 and earlier versions for Linux
Adobe AIR desktop runtime 14.0.0.178 and earlier versions
Adobe AIR SDK 14.0.0.178 and earlier versions
Adobe AIR SDK & Compiler 14.0.0.178 and earlier versions
Adobe AIR 14.0.0.179 and earlier versions for Android

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

Memory corruption vulnerabilities that could lead to code execution (CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, CVE-2014-0552, CVE-2014-0555).
A vulnerability that could be used to bypass the same origin policy (CVE-2014-0548).
A use-after-free vulnerability that could lead to code execution (CVE-2014-0553).
A security bypass vulnerability (CVE-2014-0554).
A heap buffer overflow vulnerability that could lead to code execution (CVE-2014-0556, CVE-2014-0559).
Memory leakage vulnerabilities that could be used to bypass memory address randomization (CVE-2014-0557).

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user access.

RECOMMENDATIONS:

The following actions should be taken:

Install the updates provided by Adobe immediately after appropriate testing.
Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
Do not open email attachments from unknown or untrusted sources.
Limit user account privileges to those required only.

REFERENCES:

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-21.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0547

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0548

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0549

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0550

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0551

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0552

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0553

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0554

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0555

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0556

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0557

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0559